第 37 卷第 6 期 计算机应用研究 Vol. 37 No. 6
录用定稿 Application Research of Computers Accepted Paper

基于区块链信用体系的分布式数字版权管理机制 *

周如月，钱 良

(上海交通大学 无线通信技术研究所，上海 200240)

摘 要：为了提升数字版权管理机制的效率，为去中心化内容分发网络中的版权保护问题提供解决方案，提出一种基于区块链信用体系的分布式 DRM（digital right management）机制。利用区块链增信体制及智能合约技术，该 DRM 机制设计了去中心化分布式网络环境中的版权交易过程，实现版权交易过程的不可逆加密记录，并针对内容分发应用的实际需求对分布式账本的数据结构作出轻量化调整。仿真测试和结果分析表明，基于该机制可为构建出高性能低开销的分布式内容分发系统提供技术支撑，并且相较于传统 DRM 机制该机制具备高度的灵活性和可扩展性。

关键词：数字版权管理；区块链；内容分发网络；有向无环图

中图分类号：TP37 doi: 10.19734/j.issn.1001-3695.2018.11.0870

Blockchain based digital right management for distributed content delivery network

Zhou Ruyue, Qian Liang

(*Institute of Wireless Communication Technologies, Shanghai Jiao Tong University, Shanghai* 200240 ,*China*)

Abstract: In order to improve the efficiency of Digital Right Management mechanism and provide solutions to copyright protection in decentralized content delivery networks, this paper proposed a distributed DRM mechanism based on blockchain. The mechanism designed procedures of copyright transactions in decentralized environment and made adjustment to data structure in blockchain according to demands of content distribution application. Simulation results demonstrate that the proposed mechanism can support DRM system effectively with only 6.7% overheads. Moreover, compared with traditional DRM mechanism, the proposed mechanism is of high scalability and flexibility.

Key words: digital right management; blockchain; content delivery network; directed acyclic graph

0 引言

数字版权管理技术[1]提供内容分发后的数字版权保护和对内容有效的控制方法。对于依托中心化的内容分发网络（CDN）来进行内容分发的传统数字版权管理机制来说，效率和成本很大程度上受 CDN 网络中服务器的带宽所制约，尤其是面临大量内容分发需求的场景时。中心化的数字版权管理方法不仅导致效率低下、成本较高，还易造成内容版权信息的泄露。

此外，DRM 系统需要足够灵活地能支持现有的业务模型并可扩展以适应于未来的业务模型。基于分布式结构设计的 DRM 系统具有高度的可扩展性和灵活性。在一些去中心化的网络结构中，如 D2D 网络[2,3]，数字版权管理问题仍然是一个亟待解决的问题。分布式的 DRM 机制也可为这些去中心化的网络结构提供版权管理的有效解决方案。

区块链[4]是由不可信节点基于一种全新的去中心化协议下维护的分布式数据库系统，能够安全地存储交易数据或者其他数字资产信息。区块链中的不可伪造和窜改，无须任何中心化机构的参与，具有实现理想化数字版权管理机制的潜力[5,6,7]。本文提出了一种基于区块链信用体系的分布式 DRM 机制，基于提出的 DRM 机制，可以构建出一种架构灵活、高性能、低成本的分布式内容分发系统，在支持数字版权保护的同时满足大量内容分发的需求。仿真结果表明，在分布式内容分发网络中引入该机制仅会带来 6.7%成本开销的增加。

1 序章

1.1 数字版权管理机制中的区块链关键技术

区块链是随着比特币等数字加密货币的日益普及而兴起的一种全新的去中心化基础架构与分布式计算范式。区块链技术具有去中心化、集体维护、安全可信等特点[8]。区块链的基本结构如图 1 所示。区块链是由去中心化系统中各节点共享的数据账本，每个分布式节点都可以通过特定的算法和数据结构将一段时间接收到的交易数据封装到一个带有时间戳的数据区块中，并链接到主区块链上。

在数字版权管理领域的应用中，区块链技术安全可信、去中心化、集体维护和可溯源等核心技术特征，能够为版权保护的结构性问题提供解决思路和尝试方法，带来进一步的机遇[9]。

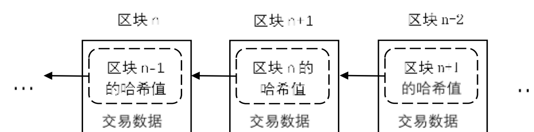


图 1 区块链的基本链式结构

Fig. 1 Structure of blockchains

收稿日期：2018-11-23；**修回日期**：2019-01-30 **基金项目**：国家自然科学基金资助项目（61771309，61671301，61420106008，61521062）；上海重点实验室基金资助项目（STCSM15DZ2270400）；数据链技术重点实验室开放基金资助项目（CLDL-20162306）；上海交通大学医工交叉基金资助项目（YG2017QN47）

作者简介：周如月（1993-），女，江苏南通人，硕士研究生，主要研究方向为无线通信（649841505@sjtu.edu.cn）；钱良（1974-），男，上海人，副教授，硕导，博士，主要研究方向为无线网络.

a) 安全可信。存储于区块链中的数据具有难以窜改的技术特征，为数字版权信息和版权交易信息提供了一种安全可信的存储方式。

b) 去中心化。区块链完全由纯数学的算法在分布式节点间建立信任关系，因此交易的产生、验证、记录、同步等活动均由分布式网络完成，达到了彻底的去中心化，网络中没有第三方中介或者权威机构参与。这意味着任何人和任何组织都可以以低廉的成本进行数字版权的注册和管理。

区块链架构的可扩展性和灵活性也体现在其具有公有链（public blockchains）、私有链（private blockchains）和联盟链（consortium blockchains）[10]三种应用模式，并可根据实际的应用需求进行相应的选择。公有链是指任何人都可读取、发送交易且交易能获得有效确认的、也可以参与其中共识过程的区块链。比特币和以太坊是其中最负盛名和最有代表性的公有链。联盟链是指由某个特定群体的成员和有限的第三方共同参与管理的区块链，由授权的用户节点共同记录交易数据，并且只有这些得到授权的成员能够对联盟链中的数据进行读写和发送交易。根据不同的应用场景账本规模不尽相同，但通常远小于公有链。私有链只对单独的个人或者实体开放，并不适合应用于数字版权管理上，文中提出的数字版权管理机制是基于公有链和联盟链的应用模式上。

1.2　基于区块链技术的智能合约

智能合约的概念最早是在 1994 年由学者 Szabo[11]提出，并将智能合约定义为“执行合同条款的计算机交易协议”。Szabo 建议将合同条款翻译成代码，并将其嵌入到能够自我执行的硬件或者软件中，以便最大限度地减少交易各方之间对可信中介的需求。由于计算手段的落后和应用场景的缺失，智能合约并未引起广泛的关注。

区块链技术的兴起重新定义了智能合约。智能合约作为一种嵌入式程序化合约，内置在区块链上。具体来说，智能合约是一组情景——应对型的程序化规则和逻辑，是部署在区块链上的去中心化、可信共享的代码程序。智能合约封装了预定义的状态及其转换规则、触发合约执行的情景。智能合约的运作机理如图 2 所示。部署在区块链上的智能合约同样具有区块链数据的一般特征，如分布式记录、存储和验证，不可窜改，可以不依赖任何中心机构进行可信交易的处理。智能合约的可编程特性使得签署方可以增加任意复杂的条款。基于智能合约，数字版权交易和支付问题可得到高效的解决方法，在提高交易效率的同时，还能有效地减少商业欺诈和双花的可能性。

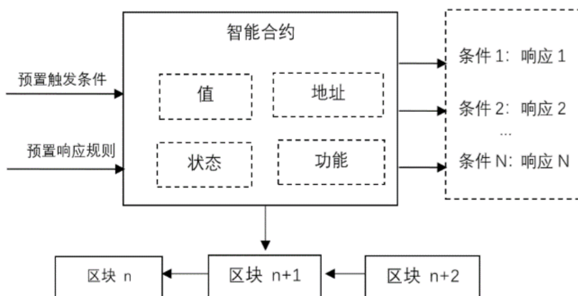


图 2　智能合约的运作原理

Fig. 2　Rationale of smart contracts

1.3　无链分布式账本

最近无链货币[12,13]成为区块链研究中一个非常有前景的研究方向。在无链分布式账本的实现中，传统区块链的链状结构和其共识算法被基于有向无环图（directed acyclic graph，DAG）的数据结构和交叉认证机制所取代。其基本思想是，为了在分布式账本中发布自己的交易，用户必须做一些工作量证明来验证其他一些未被验证的交易，检验是否存在交易冲突和双花的问题，确认之后将自己的交易指向验证的交易并加入分布式账本中。

图 3 展示了 DAG 结构中的存储单元[14]。记有向无环图为 $\Gamma=(V,E)$，其中：V 是有向无环图的顶点集合；E 为有向边集。在分布式账本的数据结构中，有向图的顶点（$v\in V$）表示交易区块，而有向边 $e=(v_1, v_2)\in E$ 表示交易区块之间的证明关系。DAG 结构通常从被称为创世区块（G）的根节点开始建立，并根据预先设定的精确规则演化。

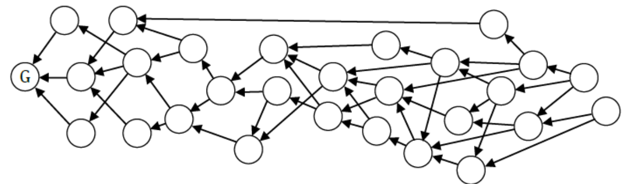


图 3　DAG 结构存储单元

Fig. 3　Storage units connected into DAG

与需要大量计算资源挖矿，交易确认延迟极高，且手续费不断增加的传统区块链结构相比，无链分布式账本的存储结构和交易验证方法具有以下若干优势，使得其具有应用于大规模内容分发网络的可能。

高吞吐量：区别于传统区块链整个网络中只能同时存在一条单链的数据结构以及出块无法并发执行的工作量证明机制，DAG 是由交易单元组成的网络，支持异步并发写入交易。高吞吐量的特性能很好地满足内容分发网络对高频版权交易的需求。

低能耗：DAG 结构中的验证是由分布式节点之间互相交叉验证完成的，没有挖矿机制，对内容分发网络中计算资源有限的设备，如移动终端、传感器等设备相当友好。

无交易手续费：由于 DAG 中的共识哲学“为了在分布式账本中发布自己的交易，用户必须做一些工作量来验证其他一些未被验证的交易”，所以整个网络中没有矿工存在，因此不对交易收取手续费。基于此特性，文中提出的基于区块链的分布式 DRM 机制能够以低廉的成本运行。

交易确认延迟低：因为 DAG 网络的存储结构，节点无须验证所有交易，仅需验证自己选择的少量交易及其父交易。如此一来，用户仅仅验证了 DAG 结构中的一部分，当其他用户选择并验证不同的交易和路径，完整的协同验证就出现了。低交易确认延迟能很好地满足 DRM 机制对即时性的需求。

考虑到传统区块链单链结构较低的交易效率和较高的交易延迟等问题，文中采取 DAG 数据结构的分布式账本技术对版权交易相关数据进行存储和验证。

2　基于区块链信用体系的分布式数字版权管理机制

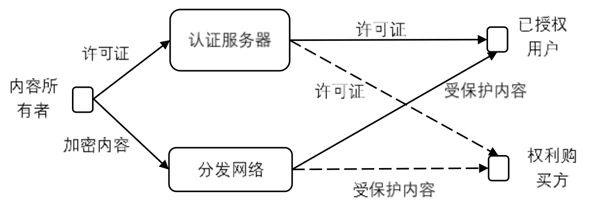
本章详细介绍了基于区块链信用体系的 DRM 机制的策略和实现细节。DRM 机制与区块链技术之间可以互相补足和结合，很大程度上是因为 DRM 机制设计的主要特征之一就是版权交易过程和内容分发过程的分离。依托区块链的技术特征，版权交易的信息可以被安全可靠地记录下来且可以轻松溯源，而内容分发过程可以依托“超级分销”（super distribution）的方式变得更加的高效。

2.1　基于区块链信用体系的 DRM 机制结构综述

在提出的 DRM 模型中涉及的实体有内容数字版权的所有者（content owner）；权利发布方（RI）和权利购买方（RC）。

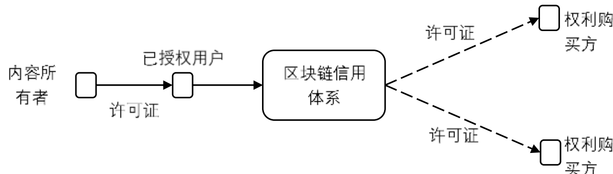
上述所有的实体都以点对点的组网方式进行连接，且节点内嵌智能合约及分布式账本。

如图 4 所示，区别于传统的 DRM 结构体系中版权购买方只能从集中式的认证服务器处得到授权的方式，在基于区块链的分布式 DRM 机制中，版权购买方可以从已获得版权的权利发布方处获得内容的授权。所有发生在购买方和发布方之间的交易信息均会以不可窜改、安全可信的方式记录在区块链中，同时内容所有者也能从上述交易中获取相关内容的版权费用，所以不存在任何侵权行为。不仅解决了传统 DRM 机制效率受制于中心服务器带宽的问题，且在降低内容分发成本的同时提高了分发效率和架构的灵活性。



(a)传统 DRM 机制架构

(a) Traditional DRM mechanism architecture



(b) 基于区块链信用体系的 DRM 机制架构

(b) DRM mechanism architecture based on block chain credit system

图 4　传统 DRM 机制架构与基于区块链信用体系的 DRM 机制架构对比

Fig. 4　Comparison between traditional DRM architecture and proposed DRM architecture

利用区块链的智能合约，该分布式 DRM 机制可以实现一种高效的内容分发激励机制。根据智能合约的预设条件和规则，一笔版权交易的费用可以包含多个转账对象、版权拥有者和权利发布方等。为权利发布方支付一部分的费用可以激励用户贡献自己的带宽资源和内容资源；同时，对于大部分原先采取 C/S 架构进行内容分发的版权所有方来说，这样的架构在帮助数字版权管理盈利的同时节省了中心服务器带宽资源的支出，减轻了中心服务器的压力，提高了服务质量。

2.2　区块链中的数据存储模式

本质上，区块链是一种可用于数据存储、数据传输和数据共识的分布式数据账本。本文采用 DAG 数据结构的分布式账本对版权交易数据进行存储和利用；同时，为了将区块链技术应用到 DRM 机制中，本文需要在单个数据区块的存储结构中加入内容信息和数字版权交易的信息。

区块链中的数据存储模式如图 5 所示。除了用于实现数据区块链接的区块头，内容信息和版权交易信息均需要被嵌入到数据区块体中。区块头存储着区块的头信息，包含父区块的哈希值、本区块体的哈希值以及时间戳等。在 DAG 的数据结构中，一个区块可能会指向多个数据区块，其指向的父区块的哈希值均包含在区块头内。区块体中，内容信息包含内容的版权信息和数字内容摘要。考虑到分布式系统中不可信节点的存在，分发内容的完整性和一致性需要在版权转移前予以确认，单向哈希函数生成的数字内容摘要可以用于内容校验和检测数据的损坏情况。版权信息通常包含内容创作者或者版权所有方的公钥地址等信息。而版权交易信息则应当准确无误地保存版权交易双方的公钥地址和其余一些交易信息。

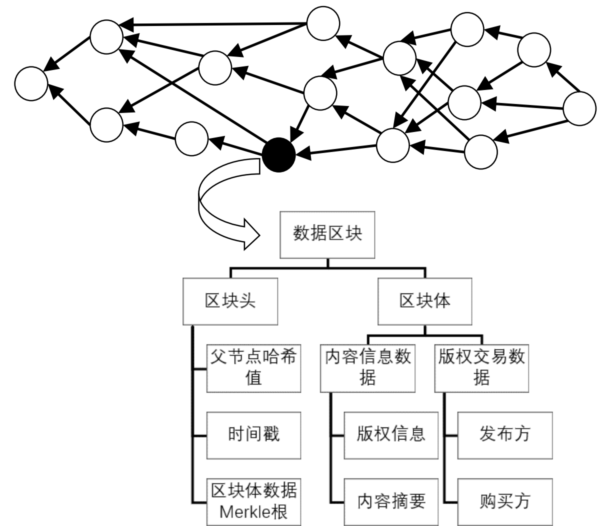


图 5　区块链数据存储模式

Fig. 5　Information storage schema in blockchain

使用上述的区块链数据存储模式可以带来诸多优势：a)所有的交易参与者都可以追踪账本中的每笔交易，确认哪些内容转发者是已经得到合法授权的，以此来杜绝无版权转发的情况；b)数字摘要技术可以保证分发内容的完整性和一致性；c)利用区块链中的数字签名技术，不仅可以减少欺诈交易的行为，也可以用于给特定的授权对象转让许可证。

2.3　数字版权分发过程

考虑到分布式环境下恶意节点的存在，本文以在去中心化环境中的两个节点——权利发布方 RI 和权利购买方 RC 的版权交易行为来展现权利转让的流程。

图 6 展现了基于区块链信用体系的版权交易的流程。

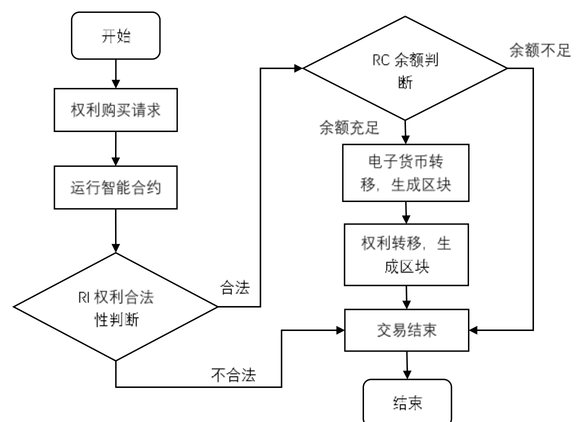


图 6　权利转让流程

Fig. 6　Flow chart for license distribution

a) 首先，在版权交易之前，为了杜绝无版权交易行为的发生，需要进行判断权利发布方是否获得合法的权利。为此，权利发布方需要提供自己获得合法权利的区块哈希值。

b) 运行智能合约，向节点内置的预先定义的智能合约模块提交该区块哈希值并运行智能合约在账本中查找该交易区块，确认 RI 授权的合法情况以及 RC 的电子货币账户余额情况。

c) 在确认 RI 授权的合法性以及 RC 的账户余额足够支持此次交易之后，智能合约改变内置的状态并通过产生新的

交易区块来更新状态。购买方账户中用于支付版权费用的电子货币被冻结，直到交易完成或交易失败。同时购买方需要提供新产生的包含权利购买信息的区块哈希值。

d) 权利发布方接收到该区块哈希值后，向节点内置的预定义的智能合约模块提交该区块哈希值并运行智能合约在账本中查找该交易区块，确认支付情况之后，智能合约改变内置的状态并通过产生新的交易区块来更新状态。同时，权利发布方为购买方签发权利实体文档。

至于权利实体的生成，考虑到分布式环境下权利保护的需求，将权利实体文档内容，以及经过权利发布方签名的文档内容转让给 RC，许可证中的一些具体内容如图 7 所示。对内容加密密钥 CEK 使用购买方的公钥进行加密保证了许可证可以被唯一地绑定到一个目标用户，只允许该目标用户使用该权利和相应的加密 DRM 内容，并且通过对权利内容的签名来保证权利实体的完整性。

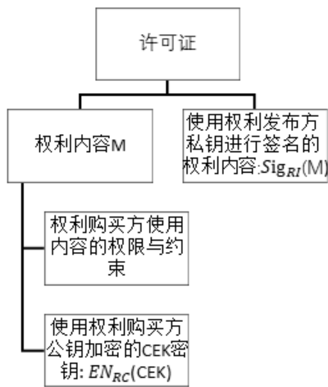


图 7　许可证结构

Fig. 7　Right object

在上述过程中，大部分的区块链开销都是由智能合约在分布式账本中查找特定交易区块而产生的，所以在该机制中的区块链开销很大程度上与账本规模有关。本文在分布式账本中构建了基于红黑树结构的唯一索引用于检索交易区块，该算法最差的时间复杂度为 $O(\log N)$ 。

2.4　DRM 方案安全性分析

对于去中心化分布式环境中的 DRM 机制而言，机制的安全性至关重要。下面分别对上述 DRM 机制中的内容对称加密算法的安全性、许可证管理的安全性以及智能合约的公平性等方面对该方案的安全性和公平性进行分析。

在该 DRM 方案中，内容拥有者在上传资源时，对资源内容采用对称加密算法中的 3DES 算法[15]，所用密钥的总长度为 192 位，其中包括 168 位有效数据位和 24 位数据校验位。由于 3DES 算法具有极高的安全性，到目前为止，除了穷举搜索法对 3DES 算法进行攻击外，还没有发现更有效的办法[16]。这就意味着 168 位有效数据位的密钥的穷举空间为 2^{168}，凭借现有攻击者的计算能力在有意义的时间范围内破解 3DES 算法的密钥几乎是不可能的。

从上面的论述可知，在无法获得 DRM 内容的加密密钥时，攻击者几乎不可能在有意义的时间内破解加密密钥，获得价值内容的访问和使用权。因此，在系统中针对内容解密密钥的保护变得极其重要，密钥管理的安全性决定了 DRM 机制的安全性。

为了发挥分布式网络在资源共享和内容分发方面的优势，网络中分发的同一内容采用的是相同的加密方式，而资源内容的解密密钥则通过用户的公钥对其加密之后包含在许可证中，无论用户以何种方式获取资源，在没有许可证的情况下都无法访问相应的内容。

考虑许可证泄露的问题，如果发放给合法用户 A 的许可证被非法用户 B 中途截取或者合法用户 A 将许可证复制给非法用户 B 使用，用户 B 仍然无法通过该许可证访问资源内容，因为许可证中的解密密钥是经过合法用户 A 的公钥进行加密的，所以即使用户 B 获取了许可证，其客户端仍然无法提取有效的私钥来解密资源内容的解密密钥。

除了技术手段之外，该 DRM 方案辅助采取经济激励的措施提高许可证管理的安全性。由前文可知，一笔版权交易的费用可以包含多个转账对象，权利发布者可以通过权利的转发和贡献自身的带宽资源获得经济利益。但是所有合法交易前，权利转发方需要向智能合约验证自身权利的合法性后才能进行权利转发。在经济激励机制的作用下，用户会更加倾向于采用合法方式获取内容版权，以便之后能够通过合法的方式进行盈利。

从以上分析可知，通过上述 DRM 内容加密方式和许可证管理方法，保证了资源内容不被非法使用的同时，也降低了非法用户恶意泄露密钥的可能，保证了方案的安全性。

DRM 机制的核心是内容权利的控制，所以涉及权利转让的版权交易过程也决定了方案的安全性和公平性。文中描述的权利转让流程是利用智能合约实现的，将权利合法性验证、权利转让、数字货币支付等功能封装在智能合约中自动执行。现存的各类智能合约及其应用本质逻辑大多是根据预定义场景的“IF-THEN”类型的条件响应规则，文中采用的也是这样的规则，智能合约判断权利合法性及购买方账户余额情况（IF）之后执行货币和权利的转让（THEN）。智能合约具有自治和去中心化等特征：版权交易一旦启动智能合约就会自动运行，不需要权利发布方和权利签署方的干预；智能合约是由去中心化存储和验证的程序代码而非中心化实体来保障执行，一旦智能合约通过判定交易成立，版权交易的双方均无法干预交易的执行情况，能够很大程度上保证交易的公平和公正性[4]。

3　仿真实验结果与分析

本章详细叙述了仿真实验的细节和相关结果分析。实验利用开源的区块链技术 Hyperledger Fabric[17]及其内置的智能合约模块，通过在开源项目的测试网络中构建内容分发过程来验证该数字版权管理机制的可行性和有效性。通过一系列的测试和应用，证明该机制可以很好地服务于分布式环境下数字内容的版权控制和完整性验证。完成可行性验证后，实验通过 NS3 仿真进一步分析该机制的效率和开销。

3.1　仿真实验

如图 8 所示，仿真环境由 CDN 服务器和一些分布式对等网络节点所组成。文章之前所提及的智能合约模块和区块存储模块均内置于对等网络节点中。

仿真实验关注平均请求响应延时（response delay per request）来评估网络的性能和分析分布式 DRM 机制的开销。请求响应延时是与用户对于服务质量的感受直接有关的一个非常重要的衡量标准。

图 9 展示了引入文中提出的 DRM 机制的分布式网络中的请求响应延时分解图。请求响应延时主要由网络响应时间 N1、N2 及引入 DRM 机制带来的时间开销组成。在仿真场景中，本文将网络响应时间归结为链路成本（link cost）带来的开销，CDN 网络和分布式网络中均有链路成本带来的开销。另一方面，在分布式网络引入该 DRM 机制所带来的时间开销主要是由在区块链中检索特定的区块数据产生的

（blockchain cost）。通常情况下，链路成本由大量复杂的因素所决定，如带宽、链路距离等。所以在效率分析中，本文将 CDN 网络的链路成本做归一化处理，将其设置为 1，而考虑到分布式 CDN 网络中的节点以点对点的方式进行连接，相对于连接至 CDN 服务器的链路成本较小，将分布式网络的链路成本设定为小于 1 的常数。链路成本比例的定义如下：

$$Link\ cost\ ratio = \frac{link\ cost\ of\ CDN}{link\ cost\ of\ Distributed\ networks}$$

为了探究在不同链路成本比例下 DRM 机制所带来的开销情况，仿真中分布式网络的链路成本被分别设置成 0.5 和 0.1。同时，中心架构的 CDN 网络的服务器被设置为每秒最多能处理 400 次请求。

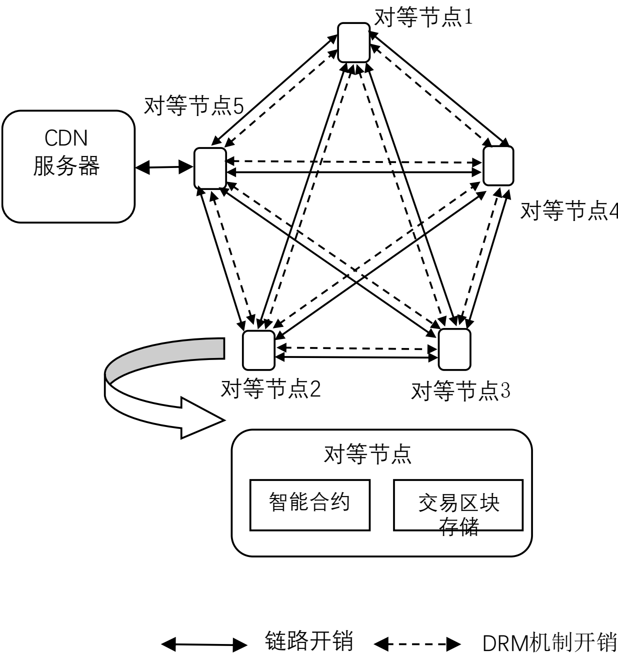


图 8　仿真实验环境

Fig. 8　Simulation scenario

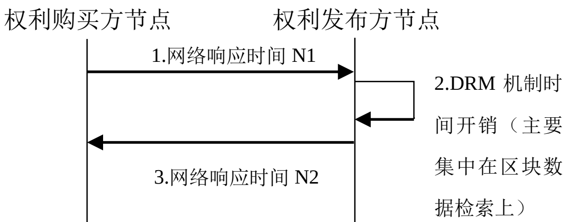


图 9　分布式内容分发网络请求响应延时分解图

Fig. 9　Response delay for distributed architectures with proposed DRM mechanism

3.2　仿真结果分析

图 10 和 11 描述了在不同链路成本比例下，CDN 网络架构、未应用 DRM 机制的分布式内容分发网络以及应用了文中提出的 DRM 机制的分布式内容分发网络之间的响应延时比较。为了验证本文提出的 DRM 机制可以支持任意区块链应用模式对应的技术架构，分别引入 10 000 交易量的联盟链账本、1 000 000 交易量的联盟链账本以及 320 000 000 交易量的公链账本作为区块链开销。

因为有限的带宽资源和服务器性能，在中心架构的 CDN 网络中，平均响应时延会随着网络中每秒请求数量（request per second，RPS）的增加而呈线性增长。当每秒请求数超过服务器能处理的请求上限时，未能及时处理的请求就会进入排队队列中等待处理，所以 CDN 曲线存在拐点。在分析引入 DRM 机制所带来的开销时，本文将未应用 DRM 机制的分布式内容分发网络架构的性能曲线作为基准曲线来对比分析。在面临大量内容分发需求时，即当每秒请求数足够大时，分布式内容分发架构的曲线会收敛于一个特定值，通过与未应用 DRM 机制的基准曲线相比，就可以得到应用 DRM 机制所带来的开销。

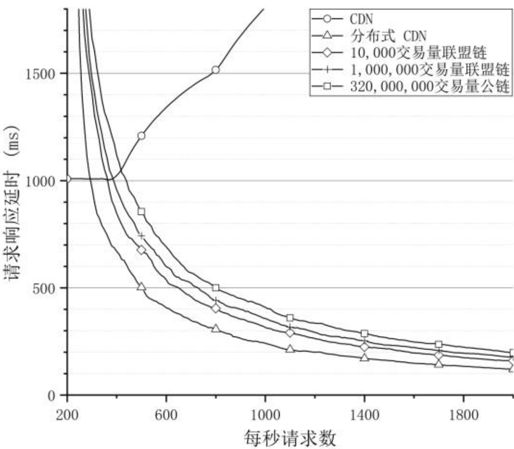


图 10　链路成本比例为 1/0.1 的请求响应延时对比

Fig. 10　Response delay comparison with link cost ratio of 10

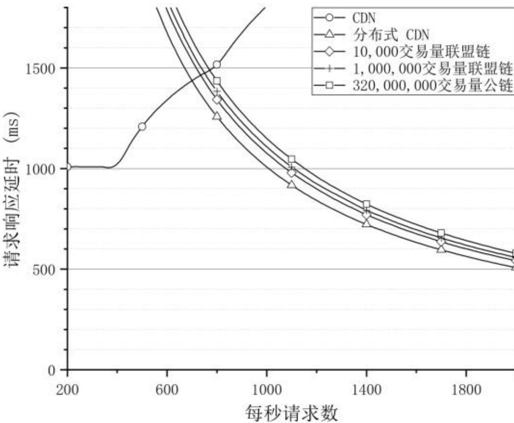


图 11　链路成本比例为 1/0.5 的请求响应延时对比

Fig. 11　Response delay comparison with link cost ratio of 2

具体的开销分析如表 1 所示。

表 1　DRM 机制开销分析

Table 5　Blockchain cost analysis

区块链应用模式	账本交易数量	链路成本比例	DRM 机制时间开销
公有链	比特币实例328,945,333	1/0.1	32.2%
		1/0.5	14.2%
联盟链	10,000	1/0.1	15.4%
		1/0.5	6.7%
	1000,000	1/0.1	22.7%
		1/0.5	10.2%

从仿真结果分析中可以得出如下结论：

a）当内容分发网络面临大规模内容分发需求时，与传统集中式的 CDN 网络相比，分布式内容分发网络在性能上更有优越性：当 RPS 大于某个特定值时，集中式 CDN 网络的请求响应延时开始大于分布式内容分发网络下的请求响应延时。

b）文中提出的 DRM 机制可为分布式环境下数字内容的版权管理提供高效的解决方法：当链路开销比例为 1/0.5 时，

基于 10 000 交易量的联盟链架构的 DRM 机制只需要 6.7%的开销，就能够有效地支持数字版权管理系统。

c）通常情况下，基于公链的 DRM 机制所引入的开销会远远大于在联盟链的环境下所带来的开销。最坏的情况下，以目前最大体量的公链应用比特币的账本规模为例，开销可高达 32.2%。幸运的是很少有实际应用需要处理像比特币那样庞大的交易数量。

4 结束语

区块链技术为分布式系统所带来的增益是当前研究的热点，也是近年来发展迅速且极具前景的研究方向。但是就分布式系统中实现区块链技术的工程成本，尚未见全面系统的分析。本文选择了分布式内容分发架构的场景，提出了基于区块链信用体系的分布式数字版权管理机制，可以支持任何媒体的认证和可信分发，在电影发布、自媒体发布等领域具备极大的商业价值和应用前景，同时文章也是首次系统全面地对区块链技术的实施架构进行了设计与性能分析。仿真结果和实验分析表明，该机制能以极低的开销高效地支持完全分布式环境下的数字内容版权管理。同时，所提出的机制可以支持任意区块链处理模式对应的技术架构，具备在不同的区块链认证环境下的架构灵活性和可实现性。

参考文献：

[1] Kamperman F L A J, Jonker W, Lenoir P J, *et al*. Digital rights management method and system: U. S. Patent 9, 843, 834 [P]. 2017-12-12.

[2] Pedersen M V, Fitzek F H P. Mobile clouds: the new content distribution platform [J]. Proceedings of the IEEE, 2012, 100 (Special Centennial Issue): 1400-1403.

[3] Wen S, Zhu X, Lin Z, *et al*. Optimization of interference coordination schemes in device-to-device (D2D) communication [C]// Proc of the 7th IEEE International ICST Conference on. Communications and Networking in China . 2012: 542-547.

[4] Swan M. Blockchain: blueprint for a new economy [M]. [S.l.]: O'Reilly Media Inc, 2015.

[5] Savelyev A. Copyright in the blockchain era: promises and challenges [J]. Computer Law & Security Review, 2018, 34 (3): 550-561.

[6] Fujimura S, Watanabe H, Nakadaira A, *et al*. BRIGHT: a concept for a decentralized rights management system based on blockchain [C]// Proc of the 5th IEEE International Conference on Consumer Electronics-Berlin. 2015: 345-346.

[7] Xu R, Zhang L, Zhao H, *et al*. Design of network media's digital rights management scheme based on blockchain technology [C]// Proc of the 13th IEEE International Symposium on Autonomous Decentralized System. 2017: 128-133.

[8] 袁勇，王飞跃. 区块链技术发展现状与展望 [J]. 自动化学报，2016, 42 (4): 481-494. (Yuan Yong, Wang Feiyue. Development and prospect of Blockchain technology [J]. Journal of Automation, 2016, 42 (4): 481-494.)

[9] Zheng Z, Xie S, Dai H N, *et al*. Blockchain challenges and opportunities: a survey [Z]. 2016.

[10] https://en. wikipedia. org/wiki/Blockchain[EB/OL].

[11] Szabo N. Smart contracts n[EB/OL]. (1994). http://szabo. best. Vwh. net/smart. contracts. Html.

[12] Bottone M, Raimondi F, Primiero G. Multi-agent based simulations of block-free distributed ledgers [Z]. 2018.

[13] Boyen X, Carr C, Haines T. Blockchain-free cryptocurrencies: a framework for truly decentralised fast transactions ,Cryptology ePrint Archive, Report 2016/871 [R]. 2016.

[14] IOTA: a cryptocurrency for the Internet of things. [EB/OL] (2017). Available: www. iota. org.

[15] Patil P, Narayankar P, Narayan D G, *et al*. A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish [J]. Procedia Computer Science, 2016, 78: 617-624.

[16] Singh G. A study of encryption algorithms (RSA, DES, 3DES and AES) for information security [J]. International Journal of Computer Applications, 2013, 67 (19) .

[17] https://www. hyperledger. Org[EB/OL].